Density Evolution Analysis of Protograph-Based Braided Block Codes on the Erasure Channel

Lentmaier, Michael; Nöthen, Benedikt; Fettweis, Gerhard

Published in:
[Host publication title missing]

2010

Citation for published version (APA):
Lentmaier, M., Nöthen, B., & Fettweis, G. (2010). Density Evolution Analysis of Protograph-Based Braided Block Codes on the Erasure Channel. In [Host publication title missing] IEEE - Institute of Electrical and Electronics Engineers Inc..
Density Evolution Analysis of Protograph-Based Braided Block Codes on the Erasure Channel

Michael Lentmaier, Benedikt Nöthen, and Gerhard P. Fettweis
Vodafone Chair Mobile Communications Systems
Dresden University of Technology (TU Dresden), 01062 Dresden, Germany
Emails: {michael.lentmaier, benedikt.noethen, fettweis}@ifn.et.tu-dresden.de

Abstract—A threshold analysis of terminated braided block codes (BBCs) is presented for the binary erasure channel. Protograph based BBCs (PG-BBCs) are considered, which can be derived by lifting the Tanner graph of a tightly braided block code. They can be interpreted as GLDPC convolutional codes that are structured in a particular way. It is shown that the terminated PG-BBCs have better thresholds than their GLDPC block code counterparts. Simulation results are presented to confirm the computed asymptotic thresholds.

I. INTRODUCTION

Braided block codes (BBCs) are a convolutional version of Elias’ product codes [1], where each code symbol is protected by two component block codes [2] [3]. Similar to Gallager’s LDPC codes [4], sparsity can be introduced into the structure of BBCs to construct codes of arbitrary length and memory without changing the component codes. Such sparse BBCs can be interpreted as LDPC convolutional codes (LDPC CCs) [5] with stronger component codes, i.e., generalized LDPC (GLDPC) convolutional codes.

Like GLDPC block codes [6], BBCs can be decoded iteratively with the belief propagation (BP) algorithm. In this case, the individual component codes are decoded by a posteriori probability (APP) decoders and the resulting reliability information about the symbols is exchanged among them during the decoding iterations. Due to their convolutional structure, BBCs are suitable for continuous transmission by means of a pipeline decoding structure, analogous to LDPC CCs [5]. Simulation results show that BBCs with relatively small memory come remarkably close to the asymptotic GLDPC threshold (see Fig. 1). On the other hand, it can be observed that terminated BBCs can even outperform the thresholds of the corresponding regular GLDPC codes [3].

The aim of this paper is to show that terminated BBCs indeed have better thresholds than their GLDPC counterparts. Such a threshold analysis becomes feasible for the binary erasure channel (BEC), where explicit input/output transfer functions for the component APP decoders are available [7]. Using these functions we are able to generalize the analysis of terminated LDPC CCs in [8] [9] to the BBCs. We start with an introduction to BBCs in Section II. Then, in Section III, (G)LDPC code ensembles based on protographs are introduced and it is demonstrated how exact density evolution equations can be used for the computation of their BEC thresholds. Using these equations, a threshold analysis is performed in Section IV for terminated, protograph based BBCs. Section V concludes the paper.

II. BRAIDED BLOCK CODES

BBCs can be defined by means of an infinite, diagonally shaped array that contains the different code symbols. Analogously to product codes [1], each code symbol is protected by one horizontal and one vertical component code. The array of a tightly braided block code (TBBC), where the width is equal to the length of the component codes, is illustrated in Fig. 2. The gray-shaded area contains the already encoded symbols. At time instant $t$ the horizontal component encoder operates in row $t$ of the array. Using the symbols $\mathbf{v}_t^{(1)}$ from the left of the main diagonal together with the new information symbols $[u_{t,0}, \mathbf{u}_t^{(2)}]$, it produces the parity-check symbols $\mathbf{v}_t^{(1)}$ and stores them in the right part of row $t$. Analogously, the vertical encoder produces the parity-check symbols $\mathbf{v}_t^{(2)}$ in column $t$ by encoding the symbols $\mathbf{v}_t^{(2)}$ together with the new information symbols $[u_{t,0}, \mathbf{u}_t^{(2)}]$ and stores them in the lower part of column $t$. Repeating this procedure, the encoder slides along the main diagonal of the array as new information symbols arrive.

The output of the TBBC encoder is the infinite code...
sequence $v = [\ldots, v_1, v_2, \ldots, v_t, \ldots]$, where
\[ v_t = [u_{t,0}, u_{t}^{(1)}, u_{t}^{(2)}, v_{t}^{(1)}, v_{t}^{(2)}] \] (1)

are the symbols produced at time $t$. The rate of a TBBC is equal to
\[ R = R^{(1)} + R^{(2)} - 1, \] (2)

where $R^{(1)}$ and $R^{(2)}$ denote the rates of the horizontal and vertical component codes, respectively. Since TBBCs are convolutional codes, the code symbols $v_t$ depend not only on the new information symbols arriving at time $t$ but also on the code symbols $v_{t-1}, \ldots, v_{t-m_{cc}}$ of previous time instants. The value $m_{cc}$ defines the memory of the TBBC.

Example 1: Assume that both the horizontal and the vertical component codes are $(15,11)$ Hamming codes. Then the input vectors $[\tilde{v}_t^{(1)}, u_{t,0}, u_{t}^{(2)}]$, $i = 1, 2$, of the encoders have length 11 and the vectors $v_{t}^{(1)}, v_{t}^{(2)}$ consist of 4 parity symbols. Since $\tilde{v}_t^{(1)}$ and $[u_{t}^{(1)}, v_{t}^{(1)}]$ must have the same length, it follows that the vectors $v_{t}^{(1)}, v_{t}^{(2)}$ have length 3. The TBCC has rate $R = 7/15$ and memory $m_{cc} = 7$. The array depicted in Fig. 2 corresponds to this case.

Like a (G)LDPC code, a TBBC can be described by a Tanner graph [10]. Then each row and each column of the array is represented by a constraint node and each symbol by a variable node. A variable node is connected to a constraint node if the associated symbol participates in the corresponding component code. The Tanner graph of a TBBC with $(7,4)$ Hamming component codes is illustrated in Fig. 3. Its girth is equal to eight, which follows from the structure of the array and is true for any TBBC.

In a sparsely braided block code (SBBC), the symbols in the array do not have to be adjacent but can be spread apart from each other. Allowing such a sparse structure, the width of the array and hence the memory of the SBBC can be increased independently of the lengths of the component codes. In this paper, we take a different approach as in [3] and use the Tanner graph of a TBBC as protograph for constructing codes of arbitrary sparsity.

III. DENSITY EVOLUTION FOR PROTOGRAPH ENSEMBLES

A. LDPC Codes

Structured LDPC codes with parity-check matrices that are composed of individual permutation matrices already appeared in Gallager’s original work [4]. For such code ensembles he proposed an algorithm to construct LDPC codes of arbitrarily large girth, provided that the block length is chosen sufficiently large. In [11] it was observed that the asymptotic minimum distance ratios of these structured ensembles are the same as for the ensembles that cannot be divided into permutation matrices. Quasi-cyclic LDPC codes can be obtained if the permutation matrices are restricted to be circulants [12]. In order to obtain structured irregular LDPC codes, some of the permutation matrices can be replaced by all-zero matrices [13]. The structure of a permutation based LDPC ensemble can be represented in a compact form by means of a protograph [14].

A protograph is a bipartite graph consisting of a set of variable nodes $V_n$, with degree $J_n$, $n = 1, \ldots, N_P$, a set of constraint nodes $C_m$, with degree $K_m$, $m = 1, \ldots, M_P$ and a set $E$ of edges that connect them. The edges connected to a variable node $V_n$ or a constraint node $C_m$ are labeled by $e_{n,j}$ or $e_{m,k}$, respectively, where $j = 1, \ldots, J_n$ and $k = 1, \ldots, K_m$. The $j$-th edge of $V_n$ is connected to the $k$-th node of $C_m$ if $e_{n,j}^c = e_{m,k}$. A protograph can be represented by means of an $M_P \times N_P$ bi-adjacency matrix $B$, which is called the base matrix of the protograph. The entry in row $m$ and column $n$ of $B$ is equal to the number of edges that connect nodes $C_m$ and $V_n$.

Example 2: The base matrix of a regular LDPC code ensemble with variable node degree $J_n = 2$ and constraint node degree $K_n = 7$ is equal to
\[ B = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \] (3)

The corresponding protograph is illustrated in Fig. 4.

The parity-check matrix $H$ of an LDPC code can be derived from a protograph by replacing each 1 in $B$ by a permutation matrix and each 0 by an all-zero matrix\(^1\). An ensemble of protograph based LDPC (PG-LDPC) codes of length $N = TN_P$ is defined by the set of matrices $H$ that can be derived from a given protograph by all possible combinations of size $T$ permutation matrices. Equivalently, the protograph can be interpreted as a template for the Tanner graph of a derived code, which can be obtained by a copy-and-permute operation [14]. The protograph is lifted by replicating each node $T$ times and the edges are permuted among these replicas in such a way that the structure of the original graph is preserved. As a consequence, a density evolution analysis for PG-LDPC ensembles can be performed within the protograph.

Assume that belief propagation is used for decoding, with log-likelihood ratios (LLRs) acting as messages. In every iteration $i$, all constraint nodes and then all variable nodes are updated. The messages computed at a constraint node $C_m$ are then equal to

$$L_{q(i)}^C(e_{m,k}) = 2 \tanh \left( \prod_{k' \neq k} \tanh \left( \frac{L_{q(i-1)}^C(e_{m,k'})}{2} \right) \right),$$

(4)

where $k, k' \in \{1, \ldots, K_m\}$. The incoming messages in the first iteration are initialized by the channel LLRs of the neighboring variable nodes, i.e., $L_{q(1)}^C(e_{m,k'}) = L_{ch}(V_n)$, where $V_n$ is the variable node connected to $e_{m,k'}$. The messages computed at a variable node $V_n$ are equal to

$$L_{q(i)}^V(e_{n,j}) = L_{ch}(V_n) + \sum_{j' \neq j} L_{q(i)}^C(e_{n,j'}),$$

(5)

where $j, j' \in \{1, \ldots, J_n\}$.

For transmission over a BEC the messages that are passed between the nodes represent either an erasure or the correct symbol values 0 or 1. In this case the BP decoder is particularly simple and exact density evolution can be described explicitly. Let $q_{i}^{(i)}(e_{m,k})$ denote the probability that the check to variable node message which is sent along edge $e_{m,k}$ in decoding iteration $i$ is an erasure. This is the case if at least one of the incoming messages from the other neighboring nodes is erased, i.e.,

$$q_{i}^{(i)}(e_{m,k}) = 1 - \prod_{k' \neq k} \left( 1 - p_{i-1}^{(i-1)}(e_{m,k'}) \right),$$

(6)

where $p_{i-1}^{(i-1)}(e_{m,k'})$, $k, k' \in \{1, \ldots, K_m\}$, denote the probabilities that the incoming messages computed in the previous iteration are erasures.

The variable to check node message sent along edge $e_{n,j}$ is an erasure if all incoming messages from the channel and from the other neighboring check nodes are erasures. Thus we have

$$p_{i}^{(i)}(e_{n,j}) = \varepsilon \prod_{j' \neq j} q_{i}^{(i)}(e_{n,j'}),$$

(7)

where $j, j' \in \{1, \ldots, J_n\}$ and $\varepsilon$ is the erasure probability of the BEC.

Equations (6) and (7) are the well-known density evolution equations for the BEC [15] [16], applied to protograph LDPC codes [14]. They can be used to compute the density evolution threshold of an ensemble, defined as the maximal value of the channel parameter $\varepsilon$ for which $p_{i}^{(i)}$ converges to zero as $i$ tends to infinity.

B. GLDPC Codes

In protograph-based GLDPC (PG-GLDPC) codes [17], each constraint node $C_m$ can represent an arbitrary block code $C_m$ of length $K_m$. Assuming an LLR based BP decoder, the messages from a constraint $C_m$ to adjacent variable nodes are then given by

$$L_{q(i)}^C(e_{m,k}) = \log \sum_{v_k} \prod_{k' \neq k} \exp \left( L_{q(i-1)}^C(e_{m,k'}) - \frac{1}{2} v_k \right),$$

(8)

where $k, k' \in \{1, \ldots, K_m\}$. Here we have partitioned $C_m$ into the sets $C_m^{0}$ and $C_m^{1}$, corresponding to codewords $v$ for which $v_k = 0$ and $v_k = 1$, respectively. The message $L_{q(i)}^C(e_{m,k})$ corresponds to the $k$-th extrinsic output generated by an optimal APP decoder for component code $C_m$, which is applied to the incoming messages of node $C_m$. The variable nodes are updated according to (5) like for conventional LDPC codes. Equation (8) is equivalent to (4) if $C_m$ is a single parity-check code.

For a density evolution analysis of PG-GLDPC codes, equation (6) can be replaced by the general expression

$$q_{i}^{(i)}(e_{m,k}) = f_k^{C_m} \left( p_{i-1}^{(i-1)}(e_{m,k'}), k' \neq k \right),$$

(9)

where $f_k^{C_m}$ is a multi-dimensional input/output transfer function that characterizes the APP decoder corresponding to (8). Note that, in general, $f_k^{C_m}$ can be different for each $k \in \{1, \ldots, K_m\}$ so that the order of edges connected to node $C_m$ can affect the performance of the ensemble. A method for computing explicit expressions for the APP decoder output distributions that can be used in (9) was presented in [7]. It is

\(^1\)The entries of multiple edges between a pair of nodes are replaced by the sum of permutation matrices.
based on a Markov chain analysis of the decoder metrics in a trellis representation of the block code $C_m$.

**Example 3:** Consider a length five shortened Hamming code defined by the parity-check matrix

$$ H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad (10) $$

which can be used, e.g., as a component code of a PG-GLDPC code. For this code the extrinsic output probabilities $q_{in}$ are

$$ q_1 = p_3p_5 - p_3p_4p_5p_2 + p_2p_3p_4 $$
$$ q_2 = p_4p_5 - p_4p_3p_5p_1 + p_1p_3p_4 $$
$$ q_3 = p_1p_5 - p_1p_4p_5p_2 + p_1p_2p_4 $$
$$ q_4 = p_2p_5 - p_2p_3p_5p_1 + p_1p_2p_3 $$
$$ q_5 = p_2p_4 - p_1p_2p_3p_4 + p_1p_3. $$

These functions, when applied in the density evolution equation (9), can be used for computing PG-GLDPC code thresholds.

The output distributions are monotonic in their arguments: if one of the input erasure probabilities is decreased, the output probabilities stay constant or decrease as well. It follows that code shortening, which is equivalent to assigning infinite reliability to some of the symbols, reduces the output erasure probabilities, like it is the case for single parity-check equations.

**IV. ANALYSIS OF TERMINATED PG-BBCS**

Taking the Tanner graph of a TBBC as a protograph we can derive ensembles of protograph based BBCs (PG-BBCs). From the array representation of a BBC with memory $m_{cc}$ follows then a convolutional protograph with infinite base matrix

$$ B_{[−∞,∞]} = \begin{bmatrix} B_{m_{cc}} & \cdots & B_0 \\ \vdots & \ddots & \vdots \end{bmatrix}. $$

The $M_P \times N_P$ component base matrices $B_i$, $i = 0, \ldots, m_{cc}$, describe the edges from the $N_P$ variable nodes at time $t$ to the $M_P = 2$ constraint nodes at time $t + i$.

**Example 4:** Consider a PG-BBC derived from a TBBC with (7,4) Hamming component codes, i.e., $N_P = 7$. The component base matrices, which follow from the graph in Fig. 3, are equal to

$$ B_0 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}, $$
$$ B_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, $$
$$ B_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}, $$
$$ B_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}. $$

Observe that the sum of the component base matrices is equal to the base matrix $B$ of the corresponding GLDPC code, which is given in (3). This reflects the fact that the graph of the TBBC in Fig. 3 can be obtained by repeating the GLDPC graph in Fig. 4 and permuting the edges among several adjacent time instants.

In general, the component base matrices of a PG-BBC that is derived from a TBBC by this procedure are given by

$$ B_0 = \begin{bmatrix} 1 & i & 0 \\ 1 & 0 & i \end{bmatrix}, \quad B_i = \begin{bmatrix} 0 & 0 & e_i \\ 0 & e_i & 0 \end{bmatrix}, \quad (11) $$

where $i = 1, \ldots, m_{cc}, e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the length $m_{cc}$ vector with a one at the $i$-th position and zeros elsewhere, $0$ is the all-zero vector, and $i$ the all-one vector.²

Assume now that we start encoding at time $t = 1$ and terminate after $L$ time instants. As a result we obtain a block protograph with the $(2(L + m_{cc})\times N_P L)$ base matrix

$$ B_{[1,L]} = \begin{bmatrix} B_0 \\ \vdots \\ B_0 \\ B_{m_{cc}} \\ \vdots \\ B_{m_{cc}} \end{bmatrix}. $$

²In this notation we group the variable nodes in the graph slightly different from the order they are transmitted according to (1), where information bits appear first. Such a reordering has no effect on the graph structure.
For the PG-BBC in Example 4, the protograph corresponding to $B_{[1,L]}$ is shown in Fig. 5 for a termination length of $L = 10$. Observe the lower degrees of constraint nodes at the start and end of the terminated protograph. These constraint nodes are now associated with shortened component codes in which the symbols of the missing edges are removed. Note that such a code shortening is equivalent to fixing these removed symbols and assigning an infinite reliability to them.

The parity-check matrix $H$ of the block codes, derived from $B_{[1,L]}$ by lifting with some factor $T$, has $N = N_P T$ columns and $M = 2M_C T$ rows, were $M_C$ denotes the number of parity-checks of the component code. It follows that the rate of the codes is equal to

$$R_L = 1 - \left( \frac{L + \Delta}{L} \right) \frac{2M_C}{N_P}$$

for some $\Delta > 0$ that accounts for the rate loss due to the termination. As $L \to \infty$, the rate $R_L$ converges to the rate of the corresponding regular GLDPC code. Assuming full rank of $H$, the rate loss coefficient can be identified as $\Delta = n_{\text{er}}$. However, shortened component codes at the ends of the graph are causing a reduced rank of $H$ that slightly increases $R_L$. For Hamming component codes of length $N_P = 7$ and $N_P = 15$ (with $M_C = 3$ and $M_C = 4$, respectively) the coefficients $\Delta = 2$ (instead of $m_{\text{er}} = 3$) and $\Delta = 5.5$ (instead of $m_{\text{er}} = 7$) could be observed by experiments with random liftings.

The terminated PG-BBCs can be interpreted as PG-GLDPC block codes of a specific structure. The length of these codes depends not only on the lifting factor $T$ but also on the termination length $L$. For a fixed $L$, the density evolution thresholds $\varepsilon_L^*$ corresponding to codes with base matrix $B_{[1,L]}$ can be estimated by recursive application of (7) and (9) for different channel parameters $\varepsilon$. We computed these thresholds for Hamming component codes of length $N_P = 7$ and $N_P = 15$ and different termination lengths $L$. The results are given in Table I and illustrated in Figure 6, together with the Shannon limit $\varepsilon_{sh} = 1 - R_L$, which follows from (13).

<table>
<thead>
<tr>
<th>$N_P = 7$</th>
<th>$N_P = 15$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L$</td>
<td>$\varepsilon_L$</td>
</tr>
<tr>
<td>10</td>
<td>0.6737</td>
</tr>
<tr>
<td>15</td>
<td>0.8681</td>
</tr>
<tr>
<td>18</td>
<td>0.8584</td>
</tr>
<tr>
<td>20</td>
<td>0.8567</td>
</tr>
<tr>
<td>25</td>
<td>0.8562</td>
</tr>
<tr>
<td>40</td>
<td>0.8562</td>
</tr>
<tr>
<td>60</td>
<td>0.8562</td>
</tr>
<tr>
<td>80</td>
<td>0.8562</td>
</tr>
<tr>
<td>100</td>
<td>0.8562</td>
</tr>
<tr>
<td>1000</td>
<td>0.8562</td>
</tr>
<tr>
<td>$\varepsilon^*$</td>
<td>$\varepsilon^*$</td>
</tr>
</tbody>
</table>

**TABLE I**
ThRESHOLDS OF REGULAR PG-GLDPC CODES AND OF TERMINATED PG-BBCS FOR DIFFERENT TERMINATION LENGTHS $L$.

As $L$ increases, the degree distributions approach those of the corresponding regular PG-GLDPC code with the same component codes. As expected, the thresholds of the PG-BBCs are decreasing with $L$. However, after a certain termination length $L$ the thresholds approach a constant value $\varepsilon_{sh}$, which interestingly is still larger than the threshold $\varepsilon^*$ of the regular PG-GLDPC code.

This phenomenon, which can also be observed for PG-GLDPC CCs [9], can be explained by a closer inspection of the structure of the terminated protograph: during the iterations, the messages along edges at times $t = 1$ and $t = L$ will be the most reliable ones because the shortened component codes at the start and end of the graph provide a stronger protection. Their erasure probabilities have the potential to converge to zero even for channel parameters $\varepsilon$ beyond the threshold of the corresponding regular GLDPC code. But when the symbols at $t = 1$ and $t = L$ are perfectly known, the connected edges can be removed from the protograph, which results in the shortened protograph $B_{[2,L−1]}$, as illustrated in Fig. 5. It follows now by induction that the messages eventually converge to zero at all times $t = 1, \ldots, L$ for arbitrary values $L$. Theorem 1 in [9], for which a proof can be found in [18], is based on the same arguments and can be generalized to the considered PG-BBCs.

Simulation results of a PG-BBC in comparison with its GLDPC counterpart are shown in Fig. 7, together with the corresponding thresholds. In this example, a relatively large termination length $L = 1000$ was chosen to demonstrate that the performance is dominated by the special structure of the protograph and not by its degree distribution alone. Motivated by the arguments above, the decoder was operating on a sliding window to reduce the required number of updates per node. Figure 8 shows the influence of $L$ on the performance of PG-BBCs. It is demonstrated that a short $L$, which causes a substantial rate reduction, can be used intentionally for improving the performance.
We considered a class of protograph based BBCs that are constructed by lifting the Tanner graph of a TBBC. These PG-BBCs can be terminated, resulting in some specially structured PG-GLDPC block codes. Based on exact density evolution equations for PG-GLDPC codes, which can be derived for the case of the BEC, we performed a threshold analysis of the terminated PG-BBCs. It turns out that the terminated PG-BBCs have better thresholds than their regular GLDPC counterparts, even for large termination lengths where the degree distributions become nearly identical. Simulation results confirm the calculated asymptotic thresholds.

The authors are grateful for the use of the high performance computing facilities of the ZIH at TU Dresden.

**REFERENCES**


